

SYSTEM AND METHOD FOR BIOLOGICAL AUTHORIZATION FOR FINANCIAL TRANSACTIONS

CROSS REFERENCE TO RELATED APPLICATIONS

1. This application claims priority under 35 U.S.C. § 119(e) from provisional application number 60/177,235, filed January 20, 2000. The 60/177,235 provisional application is incorporated by reference herein, in its entirety, for all purposes.

INTRODUCTION

2. This application relates generally to the authorization of funds electronically. More particularly, the present invention provides a system and method for selectively authorizing user-specified amounts of money for access by third parties using biological or physiological authentication.

BACKGROUND OF THE INVENTION

3. It is frequently the case that funds may be required by dependents of a primary cardholder for legitimate purposes. For example, a child away at college may require access to funds from time to time. However the primary cardholder, for example the parent, may not wish to have the child have access to unlimited amounts of funds for fear that the privilege may be abused.

4. Another situation where funds may be required relates to domestic and foreign travel. When an individual is on foreign travel, in order to minimize the potential for fraud, specific limits may be desired to be placed upon automated teller machine withdrawals from credit cards and other financial devices.

5. What would be quite useful is to allow third parties to have access to funds subject to particular limits that can be flexibly set by a primary card or account holder. It would be further useful if the primary card or account holder can create such limitations and authorizations over a network such as the word wide web.

SUMMARY OF THE INVENTION

6. It is therefore, an objective of the present invention to allow third parties to have access to funds of a primary card/account holder (hereinafter the primary account holder).

7. It is a further objective to allow the primary account holder to flexibly set limitations on the access of funds by third parties.

8. It is yet another objective of the present invention to allow the primary account holder to specify limitations based upon dollar amounts in a particular period of time.

9. It is yet another objective of the present invention to set geographic limits associated with the travel of third parties who might potentially access the finances of the primary account holder.

10. It is yet another objective of the present invention to allow the primary account holder to flexibly set limitations on access to the primary account by third parties over a network such as for example, the world wide web.

11. It is yet another objective of the present invention to allow the primary account holder to specify limitations based upon type of merchant (Standard Industry Codes).

12. It is yet another objective of the present invention to allow the primary account holder to specify limitations based upon type of transaction (i.e. cash advance or purchase).

13. It is yet another objective of the present invention to allow authorization for access to funds in the primary account by biological and physiological authentication.

14. The present invention provides a secure infrastructure via which primary account holders are free to control access by third parties to their accounts with a great deal of flexibility.

15. The present invention is a system and method for the authorization of access by a third party to a value account controlled by a primary account holder using biological or physiological authentication. For purposes of this application, a primary account holder is the person financially responsible for the use of a particular value account.

16. The term "value account" is meant by applicant to refer generically both to credit accounts, funds accounts, or other accounts representing things or intangibles of value. Common examples of value accounts are a bank account, a credit instrument, or a line of credit with a merchant for which the primary account holder is responsible. To the extent that the primary account holder desires to authorize other persons to have access to such accounts, the present invention is useful.

17. As an example, the present invention is embodied as one or more accounts, or lines of credit, which are held in one or more banks or other credit facilities (e.g., VISA, MasterCard, American Express). A primary account holder is named as the responsible party for both depositing funds and for payment of bills incurred by the value account. The value account, residing in some form of financial institution, is electronically connected to a network. The network may be private or may be an open, globally-interconnected network of networks, such as the Internet.

18. According to the preferred embodiment, the primary account holder is also connected to the same network via a communication device, such as home computer, a cellular telephone, a wireless personal digital assistant, a two-way pager, or other similar devices known in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

19. Additional objects and advantages of the present invention will be apparent in the following detailed description read in conjunction with the accompanying drawing figures.

20. Fig. 1 illustrates the architecture of a system according to an embodiment of the present invention.

21. Fig. 2 illustrates a flow chart diagram of the initial registration process by the primary account holder.

22. Fig. 3 illustrates a flow chart diagram of the process of initial authorization of third parties to the value account.

23. Fig. 4 illustrates a flow chart diagram of access to the primary account by an authorized third party.

DETAILED DESCRIPTION OF THE INVENTION

24. As noted earlier, the present invention is a system and method for allowing a primary account holder to authorize third parties to access a value account subject to flexible limitations set by the primary account holder.

25. Referring to **Fig. 1**, the architecture of the present invention is illustrated. The primary account holder registers for services according to the present invention at a registration kiosk **16**. The primary account holder allows authorization by password for

Internet access to accounts. The primary account holder has access to a workstation or personal computer **14** that is connected via a network (preferably, but without limitation, including the Internet) to the central database **12**.

26. Optionally, a biological identification device (BID) **28** is connected to the primary account holder's personal computer **14**. This biological identification device is preferably a fingerprint reader, and is alternatively embodied as a voiceprint reader, an iris recognition device, or a retinal recognition device. The BID may be embodied as any suitable biological identification device. For purposes of example only and without limitation, this BID will be discussed as a fingerprint identification device.

27. Also connected to the central database **12** via the network is a bank or financial institution **10** in which the primary account holder has his bank account.

28. The primary account holder can access and transfer funds in the value account at a financial institution **10** via a number of ways. One way for the primary account holder to gain access is via the PC **14** in conjunction with either the BID **28**, or the appropriate password. A second way is for the primary account holder to gain access via the kiosk **16** in conjunction with the BID **30**. A third way for the primary account holder to gain access is via the telephone **32** (or a wireless device) in conjunction with either the appropriate password, or the BID **22**.

29. The primary account holder can also use the PC **14**, kiosk **16**, telephone **32**, or a wireless device **34** to identify a third party (a spouse, a child, an employee, etc.) by their system ID number as being one who is allowed to have access to the value account. The third party shall have registered at a kiosk **16** (or otherwise) to obtain a system ID number. The third party's biological identity indication is represented by their system ID number,

which is preferably stored in the central database **12**. The third party performs a transaction at a merchant **24**, accessing the value account at the financial institution **10**, by reading the biological indicator on the merchant **24** BID **26**.

30. The primary account holder has the option according to the present invention of flexibly designating a variety of parameters associated with access by the third party to the value account at the financial institution **10**. For example, the basic limitation is the identification by a BID that the person attempting to gain access is the one that is authorized to access the account. This is preferably enhanced by a specific system ID number for the individual.

31. In addition to the basic authentication and limitation of the specific biological indicator, the primary account holder has the option of limiting:

- the amount that can be withdrawn at any particular time by the third party,
- a total amount that can be withdrawn during any particular period of time,
- the geographic locale from which funds may be requested,
- a range of dates over which funds can be requested by the third party,
- specific merchant types where transactions may or may not be requested, and
- other factors over which a primary account holder chooses to exert control.

32. For example, such controls enable a parent to limit the amount of money that a child attending college could obtain on a monthly basis. Extending the example, parental controls would further limit the location from which such funds could be withdrawn. If the child is supposed to be in one state, but attempts to withdraw funds from the value account when the child is located in another state, such access is denied.

33. In addition to limiting third parties, the primary account holder is empowered to limit his or her own access to the account to allow funds to be withdrawn to prevent fraud from occurring. For example, if the primary account holder is on travel in a foreign country, the primary account holder elects to allow funds to be deducted from the value account for a period of time when the person is on travel in a particular country. Accordingly, if a physical access device for the value account (check, debit card, credit card, check etc.) is lost or stolen, and then used in another country, that use could be denied based upon the geographic limitations placed on the account by the primary account holder and further denied by virtue of the fact that the biological indicator would not allow the unauthorized third party to access the funds in the first instance.

34. As part of the present invention, it is anticipated that a BID 18, associated with an ATM 20 (or other locations where funds are dispersed), is also connected via the network to the central database 12.

35. It is expected that that wireless communication of biological information will also be used with the present invention. A new generation of wireless communication devices 34 having fingerprint identification exists so that wireless communication fraud can be avoided. These wireless communication devices 34 communicate via their native wireless network and access a broader network on which the central server resides via a WAP interface 38 or other appropriate network connection. Alternatively, a wireless central server is implemented directly on the wireless network as a supplemental mirror facility to the central database. The wireless central server is programmed (for example, using WML or other wireless oriented language) for optimum interface with wireless communication devices 34.

36. Using such a wireless communication device **34**, the primary account holder has the power to authorize account parameter changes via an appropriate password or via a BID **36**. This enables the primary account holder to flexibly allow (or disallow) access to funds in the value account at the financial institution **10** by sending messages over a network to the central database **12**.

37. Referring to **Fig. 2**, the general flow of the initial registration process is illustrated. The primary account holder begins registration at a kiosk, customer service desk, or checkout lane with a BID and enters his biological indicator or indicators **120**. He is prompted to enter personal information **122**, which may simply be driver's license data read from a magnetic stripe, or include social security number, address, phone number, or any other information about the primary account holder. Then the primary account holder is asked to choose a system identification number **124**. This number may be a social security number, phone number, phone number plus one or two digits, or any other reasonably unique number easily remembered by the account holder. After the number is chosen, all data entered is transmitted to the central database **126** via a network such as the Internet.

38. The central database determines if the system identification number is unique **128**. If not, the primary account holder is prompted to choose a different number, and is offered suggestions, such as adding a digit to the previously chosen number **130**. However, absolute uniqueness of the system identification number is not strictly required to practice the invention. It is contemplated that the invention be practiced such that the system identification number need only be reasonably unique. A reasonably unique identifying number is one that has a statistically small chance of being duplicated. A reasonably

unique identifying number may also be one that is intentionally common to a small, select group of individuals, say members of a family, or partners in a business.

39. At this point, the personal information and biological identifiers will be compared to the central database for uniqueness **132**. If certain information, such as name, social security number, or biological identifiers have been previously registered the registration will be declined **134** with the reason stated with notification of how to contact central database management personnel. This contact may be immediately available at the kiosk.

40. If all information is unique, the primary account holder is prompted to enter their account information **136**. Checking account information is entered by a MICR read, an optical read, hand keying, or other method of input. Credit card or debit card information is entered by a magnetic stripe read, hand keying, or another method of input.

41. At this point, the primary account holder is prompted to enter a password, which will provide him with access to his accounts via the Internet **138**. The terminal will present a notice to the primary account holder providing authorization to access the registered accounts via the biological indicators of the primary account holder **140**. For example, the notice may state:

“I authorize the central database authority to electronically access my accounts upon presentation of my biological indicators, or presentation of my selected password over the Internet, or via a wireless communication device.”

42. The primary account holder will be prompted to enter his biological indicators **142**, to authorize future transactions. The biological indicators and account information will be transmitted to the central database **144** and recorded in the database **146**. The

terminal prints a receipt (at the primary account holder's option) giving tangible written notice of the primary account holder's authorization to access his accounts **148**.

43. Referring to **Fig. 3**, the general flow chart of the initial authorization process is illustrated. A primary account holder accesses the central database via PC **14** or kiosk **16**, chooses Value Transfer **40**, and provides identification, whether biological or otherwise **42**. If the identification is not confirmed, the transaction is cancelled **44**.

44. If the correct identification is provided, the primary account holder notes that he wishes to authorize third party access to one of the accounts **46**. At that point the primary account holder enters the third party's system identification number **48**. The primary account holder then is offered the option of setting certain limits **50** on access to the account.

45. The primary account holder is prompted to select each of the various options such as time limitations **52**. Time limitations specify whether the funds (or credit) will be available one time only, recurring (i.e., "use or lose") for a time period, recurring indefinitely, or are to accrue. Amount limitations **54** on transactions specify a predetermined threshold amount that may not be exceeded in a single transaction or an aggregation of transactions. Geography limitations **56** specify what city, state, or country transactions will be available in. Limitations as to the type of transactions **58** specify whether cash advances or merchandise only will be available. Merchant type limitations **60** might specify which Standard Industry Class (SIC) codes will be available. Once the appropriate limitations on access to funds have been specified, the transaction is completed **62**. The limitation modes listed are examples, and are not meant to limit the scope of the invention, since other limitation modes are possible.

46. It is possible for the primary account holder to allow access to multiple accounts, whereby the primary account holder sets parameters to determine which account will be accessed.

47. Optionally, the primary account holder is presented with the options of setting an order of accounts to be accessed whereby if a first account is overdrawn, then the transaction will access a subsequent account.

48. Another optional mode of operation is for the account access parameters be set up for a plurality of third parties according to a hierarchical rule system. An example of a situation where hierarchical authorization is useful is in the context of a school. The school system superintendent is authorized to spend amount X, each of the principals in the school system is authorized to spend amount X' (which is naturally smaller than amount X authorized for the superintendent), and each teacher in the school system is authorized to spend amount X'' (which is naturally smaller than amount X' authorized for the principals).

49. Referring to **Fig. 4**, access to the primary account by an authorized third party is illustrated. The third party begins a transaction **70** and the transaction amount is entered **72**. This amount may be entered by the third party for example at an ATM, or by a merchant for example at a retail store. The third party then inputs their system identification number **74**, followed by a biological identifier **76**, such as a fingerprint. The third party then picks from a menu the account to access **78**. The account menu may, for example, list Account # 1, Account #2, etc. or Checking Account #1, Credit Card #1, Credit Card #2, etc.

50. The amount, fingerprint, and system identification number are then transmitted to the central database **80**. The combination of the biological identifier and the system identification number uniquely identifies the third party **82**. If the person is not identified, the transaction is declined **84**. If the identity is confirmed, the third party's authorization to access the account is processed **86**. If the third party is not authorized to access the account chosen, the transaction is declined **88**. If the individual is authorized, the authorization parameters are compared **90**. If the transaction meets the authorization parameters the transaction is approved **94**, and a receipt is printed by the terminal **96**. If however, any parameter is exceeded, the transaction is declined and the process ends **92**.

51. As noted above, this process is preferably also used to limit account access by the primary account holder himself during the course of foreign or domestic travel, in order to limit the potential for fraud.

52. As described above, the central database functions both as a storehouse for biological identification information, and as an authorization authority that makes the automated decision (based on the primary account holder's previously recorded instructions) on transaction authorization. However, both functions need not be centralized. Instead one or both of these functionalities is optionally distributed among other devices in a network.

53. According to a hybrid embodiment, the central database continues to function as a storehouse for biological identification information. However, this central facility does not conduct transaction authorization processing. The authorization processing is handled locally at or near the location of the transaction so that the authorization processing burden is distributed around the network. When the third party initiates the transaction, providing

their system identification number and their fingerprint, only the system identification number is transmitted across the network to the central database, which returns to the local server the appropriate biological identification data for comparison to the fingerprint the third party has just provided. That local server actually makes the comparison and applies the conditions previously set by the primary account holder under which the value account may be accessed. Thus authorization is distributed while ID data is stored centrally.

54. It is also an alternate embodiment of the present invention for both authorization processing and biological ID information storage to be distributed. Operationally, this embodiment is very similar to the one previously described where authorization is distributed and ID data is stored centrally. One difference is that in the event the merchant server has the third party's biological ID information stored locally, then the merchant server proceeds directly to performing authorization processing. The only transmission to the central database server is to indicate occurrence and disposition (approved/denied) of the transaction. This data is then used for notification of the primary account holder. However, in the event that the merchant server does not have the third party's biological ID information stored locally, the merchant server then sends out a request for the information to the central database. The central database then broadcasts this request for the relevant data across the network to other facilities that store such data. The appropriate storage device responds by returning to the central database the appropriate biological identification data for relay to the merchant server or, in the alternative, transmits it directly to the merchant server. Once the biological ID information is obtained, the merchant server makes a comparison to the fingerprint the third party has just provided. Thus, both authorization processing and storage of ID information are distributed.

55. According to another hybrid embodiment, the central database stores no biological identification information but conducts all authorization processing for the system. The storage of biological identification information is handled locally at or near the location of the transaction so that the data storage burden is distributed around the network. When the third party initiates the transaction, providing their system identification number and their fingerprint, the merchant server transmits a package of information across the network to the central database. The package of information contains the system identification number provided, an extract of biological ID data from the fingerprint proffered, and (if available in the merchant server's own database) the biological identification data corresponding to the that third party, as previously recorded. In the event that the merchant server local to where the transaction is being initiated does not have a copy of that third party's biological identification data, then the central database sends out a request for the relevant data across the network to other facilities that store such data. The appropriate storage device responds by returning to the central database the appropriate biological identification data for comparison to the fingerprint the third party has just provided. That central database actually makes the comparison and applies the conditions previously set by the primary account holder under which the value account may be accessed. Thus authorization is done centrally while ID data is distributed.

56. An additional feature of the present invention is wireless notification of the primary account holder that an authorized third party has accessed an account. The wireless message (sent, for example, to a cell phone, PDA, or pager) is preferably an alphanumeric message that indicates at least the name of the party who accessed the account, and the amount of the transaction. This provides a near real time notification to the primary account holder of activity on the account.

57. Such notification is optionally made via an email message addressed to the primary account holder. Although email is not always as immediately accessible as a pager carried on one's person, the medium of email easily permits the message to include a detailed accounting of all relevant facts about the transaction, including (if desired) a listing of items bought from a merchant.

58. Another aspect of the present invention is real time authorization by the primary account holder of transactions involving the value account. This means that the transaction completion is contingent upon real time assent by the primary account holder, rather than a rule-based, automated approval/disapproval as described above. At the primary account holder's option, certain transactions are designated as requiring a real time confirmation by the primary account holder. For example, transactions that exceed a predetermined threshold amount (e.g., \$500.00), or purchases of certain predetermined types of goods (e.g., casino chips or liquor), or transactions outside a pre-approved geographic area (e.g., across the state line).

59. The real time authorization aspect of the present invention is implemented through any of a number of high tech or low tech options. One method is to request approval of the transaction from the primary account holder by sending a message to his or her wireless communication device with integrated BID. Another method is to request approval of the transaction via telephone (wireless or POTS) and then simply authenticate any approval by querying the putative primary account holder for the password.

60. A biological identification authorization system for financial transactions has been illustrated. It will be appreciated by those skilled in the art that the system and methods of the present invention can be used to authorize and prevent fraud in such areas as

telecommunications services, access to bank accounts, and financial and information transactions of many different kinds. Thus, the present invention is not limited in its utility only to access to value accounts. Specifically, the present invention has utility in preventing unauthorized access to information stored on various types of information servers.

61. The present invention has been described in terms of preferred embodiments, however, it will be appreciated that various modifications and improvements may be made to the described embodiments without departing from the scope of the invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214